PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-088322
(43)Date of publication of application : 30.03.1999

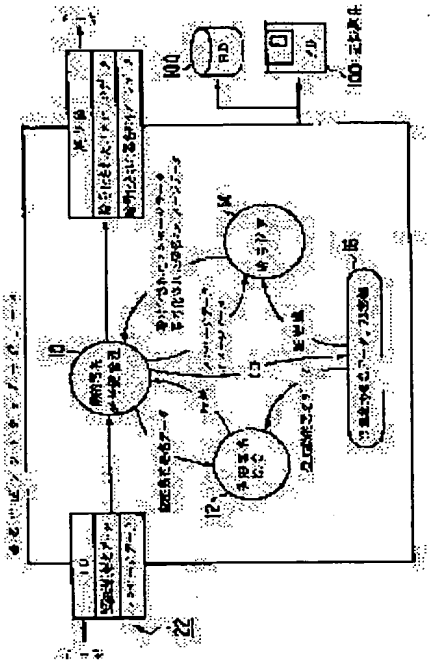
(51)Int.Cl. H04L 9/32
G06T 7/00
G09C 1/00
// A61B 5/117

(21)Application number : 09-236927
(22)Date of filing : 02.09.1997

(71)Applicant : KIYADEITSUKUSU:KK
(72)Inventor : TABUKI TAKAAKI

(54) DIGITAL SIGNATURE GENERATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a digital signature system full of convenience for easily managing a secret key in a digital signature utilizing a public key cipher system.
SOLUTION: Based on an 'ID' transmitted from a user, a dynamic signature cipher key management module 10 obtains registered dynamic signature data and the secret key from an array management module 16. The registered dynamic signature data and authentication dynamic signature data transmitted from the user are collated in a dynamic signature collation module 12. In the case of judging that both are the same signature data, the dynamic signature cipher key management module 10 supplies message data transmitted from the user and the secret key to a cipher computing module 14 and the cipher computing module 14 transmits the message data or the like ciphered by the secret key to the dynamic signature cipher key management module 10. The dynamic signature cipher key management module 10 sends back the ciphered, that is signed, message data or the like to the user. Since the secret key is buried in a program, even when the program is copied, a misuse by a third person is not invited.



LEGAL STATUS

[Date of request for examination] 09.08.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－88322

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ
Ｇ０６Ｔ	7/00		Ｇ０９Ｃ	1/00	６４０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ	15/62	４６５Ｐ
// Ａ６１Ｂ	5/117		Ａ６１Ｂ	5/10	３２０Ｚ
					３２２

審査請求　未請求　請求項の数14　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－236927

(22)出願日　平成９年(1997)９月２日

(71)出願人　591210910
株式会社キャディックス
東京都世田谷区新町２丁目26番15号

(72)発明者　田吹　隆明
東京都世田谷区新町２丁目26番15号　株式会社キャディックス内

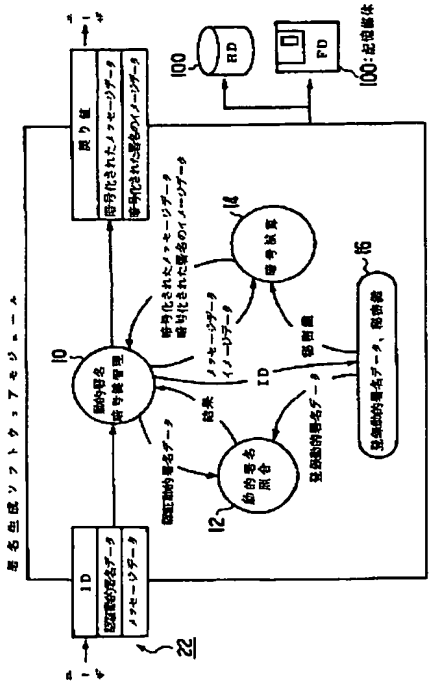
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　ディジタル署名生成方法

(57)【要約】

【課題】　公開鍵暗号方式を利用したディジタル署名において、秘密鍵の管理を容易にし、利便性に富むディジタル署名方法を実現する。

【解決手段】　ユーザから送信されてきた「ＩＤ」に基づき、動的署名暗号鍵管理モジュール１０は、配列管理モジュール１６から登録動的署名データと、秘密鍵を得る。登録動的署名データと、ユーザから送信されてきた認証動的署名データとは、動的署名照合モジュール１２で照合される。両者が同一の署名データであると判断された場合には、動的署名暗号鍵管理モジュール１０は、ユーザから送信されてきたメッセージデータを上記秘密鍵を暗号演算モジュール１４に供給する。暗号演算モジュール１４は、秘密鍵で暗号化したメッセージデータ等を動的署名暗号鍵管理モジュール１０に送信する。動的署名暗号鍵管理モジュール１０は、暗号化、すなわち署名を施したメッセージデータ等をユーザに送り返す。秘密鍵がプログラム中に埋め込まれているため、プログラムがコピーされても第三者の悪用を招くことがない。



【特許請求の範囲】
【請求項１】ディジタル署名の対象であるメッセージデータと、前記ディジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力ステップと、
前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得ステップと、
前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査ステップと、
前記検査ステップにおいて、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でディジタル署名を施すディジタル署名ステップと、
を含むことを特徴とするディジタル署名生成方法。
【請求項２】請求項１記載のディジタル署名生成方法において、
前記登録生体署名データ取得ステップは、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするディジタル署名生成方法。
【請求項３】請求項１記載のディジタル署名生成方法において、
前記登録生体署名データ取得ステップは、同一ユーザが複数の識別子を所有することを許容することを特徴とするディジタル署名生成方法。
【請求項４】請求項１、２又は３記載のディジタル署名生成方法において、
前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするディジタル署名生成方法。
【請求項５】請求項１、２又は３記載のディジタル署名生成方法において、
前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするディジタル署名生成方法。
【請求項６】請求項１、２又は３記載のディジタル署名生成方法において、
前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするディジタル署名生成方法。
【請求項７】請求項５記載のディジタル署名生成方法において、
前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換ステップと、
前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名ステップと、
を含むことを特徴とするディジタル署名生成方法。
【請求項８】ディジタル署名の対象であるメッセージデータと、前記ディジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力手順と、
前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得手順と、
前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査手順と、
前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でディジタル署名を施すディジタル署名手順と、
を含むプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項９】請求項８記載のコンピュータ読みとり可能な記憶媒体において、
前記登録生体署名データ取得手順は、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項１０】請求項８記載のコンピュータ読みとり可能な記憶媒体において、
前記登録生体署名データ取得手順は、同一ユーザが複数の識別子を所有することを許容することを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項１１】請求項８、９又は１０記載のコンピュータ読みとり可能な記憶媒体において、
前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項１２】請求項８、９又は１０記載のコンピュータ読みとり可能な記憶媒体において、
前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項１３】請求項８、９又は１０記載のコンピュータ読みとり可能な記憶媒体において、
前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。
【請求項１４】請求項１１記載のコンピュータ読みとり可能な記憶媒体において、
前記プログラムは、
前記入力された生体署名データであるデータであって、前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手順と、
前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手順と、
を含むことを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、公開鍵暗号方式に関する。特に、公開鍵暗号方式を用いてディジタル署名を行う方法に関する。

【0002】

【従来の技術】近年、ネットワークによる通信が発展し、ネットワーク上におけるメッセージの送受信等に暗号化方式が利用される場合も多い。暗号化方式には、古典的な共通鍵方式も用いられているが、鍵の管理が煩雑になる等の理由から、公開鍵暗号方式が用いられつつある。

【0003】公開鍵暗号方式においては、各人は自己の秘密鍵を秘密に管理し、自己の公開鍵を他人に公開する。そして、他人は、ある個人の公開鍵を用いてメッセージを暗号化してその個人に送る。公開鍵により暗号化されたメッセージは、秘密鍵を知っているその個人のみが復号化できるため、第三者に対してメッセージの内容は秘密に保たれる。

【0004】さらに、この公開鍵暗号方式は、いわゆるディジタル署名を容易に行うことができるという特徴を有している。

【0005】すなわち、ある甲が所定のメッセージについて自己の署名を行う場合には、そのメッセージに対して甲の秘密鍵で暗号化を行う。この秘密鍵で暗号化したメッセージは甲の公開鍵でのみ復号化できる。そのため、だれでも、甲の公開鍵でそのメッセージを復号化し、もとのメッセージの内容を確認することができる。甲の公開鍵で復号化できるのは、甲の秘密鍵で暗号化した文章だけである。従って、甲の公開鍵で復号化できたことは、甲が確かにそのメッセージに対して甲の秘密鍵を用いて暗号化したことを意味する。そして、甲の秘密鍵を知っているのは甲のみであるため、このような暗号化ができるのは甲のみである。

【0006】このように、甲のみが行える処理を他人が確認できるため、この処理をもって甲の「署名」と見なすことができる。

【0007】さて、このようなディジタル署名をはじめとして、公開鍵暗号方式においては、秘密鍵はその所有者のみが知っている必要がある。すなわち、秘密鍵は各個人が個人の責任において厳重に管理しなければならない。

【0008】ところが、近年用いられている公開鍵暗号方式に用いられる鍵の長さは、暗号強度を保つために500ビットから1000ビット程度のものが用いられ又は提案されている。

【0009】数桁程度のパスワードのようなものならばともかく、このような500ビットや1000ビット程度のデータは、人間が容易に覚えられるものではない。そこで、一般には公開鍵暗号方式の秘密鍵はコンピュータ内のハードディスクに保存したり、ICカード内に記憶させておくことがなされている。

【0010】しかし、秘密鍵をコンピュータ内のハードディスク等に格納した場合には、誰でもその秘密鍵を利用することができる可能性がある。そのため、一般にはそのハードディスク内に格納した秘密鍵は、パスワードによるプロテクトが施されている場合が多い。すなわち、その秘密鍵をディジタル署名等に使用する場合にはその利用者はパスワードを入力することにより初めてその秘密鍵を使用できるのである。

【0011】

【発明が解決しようとする課題】従来の公開鍵暗号方式の秘密鍵を利用したディジタル署名においては、このように秘密鍵の管理は各個人が行わなければならず、また、具体的にはパスワード等による秘密鍵のプロテクトが行われていた。

【0012】しかし、パスワードは、人間が覚えやすいものである必要があるため、一般には短いものが多く、不注意により他人の目に触れやすい。かつ、一旦目に触れてしまった場合（短いため）覚えられやすいという性質がある。

【0013】このように、従来の秘密鍵の保管は結局の所パスワードの強度に依存していたため、秘密鍵のプロテクトにも自ずと限界があった。その結果、第三者によるいわゆる「なりすまし」を招きやすく、第三者がその正当な権利を有する者になりすまして、ディジタル署名を行ってしまう恐れも小さくはなかった。

【0014】さらに、基本的に秘密鍵の管理は、その正当使用者個人の管理に任されている。そのため、例えば法人が使用者であるような「法人鍵」を使用する場合においても結局は個人が秘密鍵の管理を行っている。そのため、秘密鍵の重要度に関係なく、その鍵が個人の鍵であっても法人の鍵であっても、同じような安全度でしか管理されていない。

【0015】その結果、ある企業内部で、個人が重要な法人鍵を不正に使用してしまう可能性は、個人の鍵が不正に使用されてしまう可能性とほとんど変わらないのが現状である。

【0016】また、近年、企業においては法人が秘密鍵の所有者になること、すなわちその企業を表す鍵が望まれている。このような法人鍵は、いわば従来の法人の印章に相当するものである。このような法人鍵は、その法人である企業の各社員が使用する性質のものである。しかし、1つの秘密鍵を特定の個人だけが使用することを前提としている現在の公開鍵暗号方式の実現手法では、1個の法人鍵を複数人で使用する形態については何ら考慮されてはいない。このことは換言すれば1個の秘密鍵をその本人（法人）の代理人が使用する仕組みが、未だ構築されていないことを意味している。

【0017】本発明は、以上のような課題を解決するた

めになされたものであり、その目的は、企業等において、各個人がディジタル署名を行う場合に、不正な使用を確実に防止するためのディジタル署名のための方法を構築することである。

【００１８】

【課題を解決するための手段】本発明はディジタル署名のための方法に関するものであり、本発明において特徴的なことは、ＩＤやパスワードなどの他に、生体署名データを用いて各人の識別を行っているため、より正確に各個人の識別を可能としていることである。

【００１９】また、本発明において特徴的なことは、複数の秘密鍵が、複数の人によって使用され得る点にある。このようなディジタル署名の手法を実現するために、記憶手段内には、複数のユーザ対複数の秘密鍵、のデータ構造が構築されている。

【００２０】従来の技術においては、秘密鍵はあくまでも１人の人間によって所有・管理されていた。しかし、そのため、その１人のみが使用できる仕組みを構築していたので、上述したようにパスワードを盗まれることによる不正使用（なりすまし等）を招くおそれがあったのである。

【００２１】本発明は、複数の秘密鍵が複数人によって使用される方式を実現するディジタル署名生成方法を提供している。具体的には、以下のような手段を採用している。

【００２２】本発明は、上記課題を解決するために、ディジタル署名の対象であるメッセージデータと、前記ディジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力ステップと、前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得ステップと、前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査ステップと、前記検査ステップにおいて、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でディジタル署名を施すディジタル署名ステップと、を含むことを特徴とするディジタル署名生成方法である。

【００２３】生体署名データとは、個人を特定するためのいわゆるＢｉｏｍｅｔｒｉｃｓなデータであり、指紋や網膜パターンなどが使用される。特に、以下に述べる実施形態では種々のメリットがあることから署名データが使用されている。

【００２４】また、本発明は、前記登録生体署名データ取得ステップは、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするディジタル署名生成方法である。

【００２５】異なるユーザに対して同一の秘密鍵を提供することができ、例えば法人鍵などの管理を容易に行えるものである。

【００２６】また、本発明は、前記登録生体署名データ取得ステップは、同一ユーザが複数の識別子を所有することを許容することを特徴とするディジタル署名生成方法である。

【００２７】１人のユーザでも役職を複数有する場合も多い。このような場合に、役職毎にディジタル署名を変える必要がある。したがって、本発明においては同一ユーザでも複数の識別子（ＩＤとも呼ぶ）を有することを認め、１人のユーザが複数の秘密鍵を使用できるようにしている。

【００２８】また、本発明は、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするディジタル署名生成方法である。

【００２９】また、本発明は、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするディジタル署名生成方法である。

【００３０】また、本発明は、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするディジタル署名生成方法である。

【００３１】また、本発明は、前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換ステップと、前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名ステップと、を含むことを特徴とするディジタル署名生成方法である。

【００３２】イメージデータをも秘密鍵を用いて署名したので、従来の手で行う署名のイメージを利用することができ、従来のシステムとの類似性を維持することができる。

【００３３】また、本発明は、これまで述べた方法に関する発明を実現するプログラムを格納したコンピュータ読みとり可能な記憶媒体に関する。

【００３４】具体的には、以下のような手順を実行するプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【００３５】本発明は、ディジタル署名の対象であるメッセージデータと、前記ディジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力手順と、前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得手順と、前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査手順と、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でディジタル署名を施すディジタル署名手順と、を含むプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【００３６】また、本発明は、前記登録生体署名データ取得手順は、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするプログラムを格納し

たコンピュータ読みとり可能な記憶媒体である。
【００３７】また、本発明は、前記登録生体署名データ取得手順は、同一ユーザが複数の識別子を所有することを許容することを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。
【００３８】また、本発明は、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。
【００３９】また、本発明は、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。
【００４０】また、本発明は、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。
【００４１】また、本発明は、前記プログラムは、前記入力された生体署名データであるデータであって、前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手順と、前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手順と、を含むことを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。
【００４２】
【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。
【００４３】本実施の形態においては、ユーザが利用するコンピュータ上において、ユーザのＩＤ等だけでなく、ユーザの認証動的署名データに基づいて、ユーザの識別を行い、識別したユーザの秘密鍵を用いてディジタル署名を行ったものである。
【００４４】具体的には、本実施の形態は、コンピュータ上で動作するプログラムで実現されている。
【００４５】本実施の形態に係るプログラムの各モジュールの構成図が図１に示されている。この図に示されているように、動的署名暗号鍵管理モジュール１０と、動的署名照合モジュール１２と、暗号演算モジュール１４と、配列管理モジュール１６と、が本プログラムに含まれている。
【００４６】本実施の形態においては、これらのモジュールを含むプログラムを用いて、そのコンピュータのユーザの要求に応じて、所定のメッセージデータに対し署名を行っている。
【００４７】入力信号
本プログラムの具体的な動作を説明する前に、プログラムに入力する信号に関する説明を中心に本実施形態の特徴を述べる。
【００４８】このプログラムに対する入力２２は、図１に示すように、ユーザの「ＩＤ」と、ユーザの「認証動的署名データ」と、そのユーザが署名を受けたい「メッセージデータ」と、を含んでいる。本プログラムは、そのユーザの秘密鍵を用いて、「メッセージデータ」を暗号化することによって「メッセージデータ」に署名をする。そして、「暗号化された（署名された）メッセージデータ」が出力されるのである。
【００４９】ここで、認証動的署名データとは、そのユーザの「手で書いた署名」のデータや、指紋、網膜パターンなどのいわゆるＢｉｏｍｅｔｒｉｃｓな個人特定データである。本実施の形態においては、例えば、認証を利用したい者がそのコンピュータに周辺機器等として備えられているタブレット上でスタイラスペンなどを用いて「手で書いた署名」をする事により、認証動的署名データが入力される。
【００５０】さて、本プログラムの入力２２の「認証動的署名データ」とは、ユーザがディジタル署名を行いたい場合に入力した動的署名データである。上述したように、例えば端末のタブレットなどから、そのユーザの「手で書いた署名」のデータなどが、この「認証動的署名データ」として利用される。
【００５１】この「認証動的署名データ」は、配列管理モジュール１６において配列中に予め格納されている「登録動的署名データ」と、比較照合される。実際の比較照合処理は、動的署名照合モジュール１２で行われる。このように、本実施の形態においては、生体データを用いて本人であるか否かの検査を行っているので、本人以外の人間による不正なディジタル署名を効果的に防止することができる。この検査処理の流れに関しては、後において詳述する。
【００５２】また、図１に示されているように、本プログラムは、配列管理モジュール１６を有している。この配列管理モジュール１６においては、各個人（の「ＩＤ」）とその個人が使用する「秘密鍵」の管理が行われている。具体的には「ＩＤ」と、「秘密鍵」が配列中に記憶されているのである。さらに、上述した「登録動的署名データ」も、この配列管理モジュール１６において、配列中に格納されて管理されている。
【００５３】本実施の形態において特徴的なことは、秘密鍵等が、ＩＣカードなどの特定のハードウェア中に記憶されているのではなく、ソフトウェア中に組み込まれていることである。ソフトウェア中に組み込む手法は従来の種々の方法が利用可能であるが、例えば本実施の形態においては、データ配列中にユーザの「ＩＤ」や「秘密鍵」等を格納している。
【００５４】このように、ソフトウェア中に組み込まれているため、たとえ悪意の第三者に本実施の形態におけるプログラムが盗まれてコピーされても、そのプログラムを悪用すること、例えば間違ったＩＤを利用して正規の秘密鍵を利用すること等は行えない。その理由は、プログラム中に組み込まれた「ＩＤ」や「秘密鍵」の内容

を書き換えることは、そのプログラムの作成者ならば容易であるが、第三者にとっては一般に非常に困難なことだからである。

【００５５】本実施の形態において特徴的なことは、秘密鍵の管理がその所有者である個人ではなく、本実施の形態におけるプログラムが集中的に行っていることである。このような手段を講じることによって、そのコンピュータを使用する各人の秘密鍵の管理を集中して行うことができ、煩雑な秘密鍵の管理を個人が行う必要がなくなる。

【００５６】尚、本実施の形態においては、「手で書いた署名」データを利用したが、上述したようにこの動的署名データは、指紋や網膜パターンなど、Ｂｉｏｍｅｔｒｉｃｓに本人を特定しうるデータであればどのようなものでもかまわない。

【００５７】動作

次に、本発明のディジタル署名生成方法の動作について、プログラムの処理の流れを中心に説明する。

【００５８】本実施の形態におけるプログラムは、これまで述べた、ユーザの「ＩＤ」、「認証動的署名データ」、及び「メッセージデータ」から成る入力２２が供給されると、まず、動的署名暗号鍵管理モジュール１０が、そのＩＤが表すユーザに対し登録されている「登録動的署名データ」を、配列管理モジュール１６から読み出す。図１に示すように、動的署名暗号鍵管理モジュール１０は、「ＩＤ」を配列管理モジュール１６に与える。そして、配列管理モジュール１６は、この「ＩＤ」をキーとして、配列に格納されているデータの検索を行い、「登録動的署名データ」と「秘密鍵」を出力する。

【００５９】さて、配列管理モジュール１６が出力した「登録動的署名データ」は、図１に示されているように、動的署名照合モジュール１２に供給される。一方、動的署名暗号鍵管理モジュール１０も、ユーザが入力した「認証動的署名データ」を動的署名照合モジュール１２に供給する。

【００６０】動的署名照合モジュール１２は、供給された上記「認証動的署名データ」と「登録動的署名データ」との比較・照合を行う。そして、その比較の結果を動的署名暗号鍵管理モジュール１０に送信する。

【００６１】さて、配列データに格納されている「登録動的署名データ」と、ユーザによって入力された「認証動的署名データ」とがその特徴事項について一致し、共に同一人に対するＢｉｏｍｅｔｒｉｃｓな署名データであると判断される場合には、ディジタル署名の要求が正しく行われている（正規のユーザによりディジタル署名が要求されている）と判断される。したがって、この場合は上記比較結果として例えば「正常」を動的署名暗号鍵管理モジュール１０に対し送信するのである。この「正常」である旨の比較結果が動的署名暗号鍵管理モジュール１０に送信された後は、後に述べるディジタル署名の処理が、暗号演算モジュール１４において実行される。

【００６２】一方、予め配列管理モジュール１６に登録されている「登録動的署名データ」と入力された「認証動的署名データ」とがその特徴事項について一致せず、同一人に対するＢｉｏｍｅｔｒｉｃｓな署名データではないと、動的署名照合モジュール１２（図１参照）において判断された場合には、この認証の要求は不正行為によって行われた要求であると判断し、本プログラムは、ユーザの要求を拒絶する。具体的には、動的署名暗号鍵管理モジュール１０が拒絶のメッセージをユーザに送信するのである。

【００６３】さて、動的署名照合モジュール１２が、「正常」である旨の結果を動的署名暗号鍵管理モジュール１０に送信してきた場合には、動的署名暗号鍵管理モジュール１０は、暗号演算モジュール１４に対してディジタル署名処理を行わせる。すなわち、暗号演算モジュール１４は、秘密鍵による暗号化をメッセージデータに対して施すのである。

【００６４】ここで、秘密鍵は、図１に示すように配列管理モジュール１６が予め出力している。暗号演算モジュール１４は、予め出力されているこの秘密鍵を用いて暗号演算、すなわちディジタル署名を行うことができる。

【００６５】図１に示すように、暗号演算モジュール１４は、暗号化の対象である「メッセージデータ」を動的署名暗号鍵管理モジュール１０から受信する。さらに、本実施の形態においては、暗号化の対象として「メッセージデータ」だけでなく、「イメージデータ」をも暗号演算モジュール１４は受信する。そして、これら「メッセージデータ」及び「イメージデータ」の暗号化（署名）が暗号演算モジュール１４において行われる。

【００６６】この「イメージデータ」とは、ユーザにより入力された「認証動的署名データ」をイメージとして表現したイメージデータである。「認証動的署名データ」は、例えば「手で書いた署名」がユーザにより書かれる際のペンの動きをペンの速度・方向やペンの押圧力等で表した数値データである。そして、この「手で書いた署名」をイメージとして表したデータとは、その署名データ（押圧力等で表した数値データ）を人間に見える形で表すため、上記ペンの動きを２次元の紙の上に再現し、人間の視覚で把握できるようにした画像データである。

【００６７】この「認証動的署名データ」をイメージとして表現したイメージデータに変換する処理は、動的署名暗号鍵管理モジュール１０において行われる。変換後のイメージデータが図１に示すように暗号演算モジュール１４に供給されるのである。

【００６８】本実施の形態において、このような署名データのイメージデータをも暗号化している理由は、実際

に肉眼で把握できる形で文章中に署名を表示したいという要求も現実にあるからである。本実施の形態においては、このようにイメージデータをも暗号化したが、このイメージデータの暗号化は、本発明にとっては必ずしも必須の事項ではない。

【００６９】暗号演算モジュール１４は「メッセージデータ」及び「イメージデータ」を暗号化すると、得られた「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」を出力する。

【００７０】動的署名暗号鍵管理モジュール１０は、「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」をユーザに返す。これによって、ユーザは、自ら秘密鍵を管理しなくとも、容易に署名を行うことが可能である。特に、本実施の形態においてはＩＤだけでなく、Ｂｉｏｍｅｔｒｉｃｓな動的署名データを用いて、本人であることを確認したので、不正に秘密鍵を使用した署名が行われてしまうことを効果的に防止することができる。

【００７１】さらに、動的署名暗号鍵管理モジュール１０は、図１に示すようにユーザに「戻り値」をも返す。この「戻り値」は、暗号演算の結果を表すいわば「リターンコード」と呼ばれるコードの一種である。

【００７２】ユーザは、この「戻り値」の値を検査することにより、暗号演算が正常に終了したのか否か、それとも、ＩＤが表す人物について登録されている登録認証データと認証動的署名データとの特徴事項が一致しなかったのか否か、等について詳細な情報を得ることができる。

【００７３】尚、本実施の形態において、本発明のディジタル署名生成方法の各要素は、プログラムで実現されている。

【００７４】具体的には、動的署名暗号鍵管理モジュール１０は、入力ステップ等に相当する。また、動的署名暗号鍵管理モジュール１０は、動的署名照合モジュール１２との共同作用で、本発明の検査ステップを実現する。また、動的署名暗号鍵管理モジュール１０は、配列管理モジュール１６との共同作用で、本発明の登録動的署名データ取得ステップを実現する。また、動的署名暗号鍵管理モジュール１０は、暗号演算モジュール１４との共同作用で、本発明のディジタル署名ステップを実現する。

【００７５】また、動的署名暗号鍵管理モジュール１０は、イメージデータへの変換を行う本発明の変換ステップを実現する。

【００７６】さらに、本実施の形態における、上記モジュールから成るプログラムは、コンピュータが稼働していないときはコンピュータ読みとり可能な記憶媒体１００に格納されている。この記憶媒体１００は、ハードディスクを用いるのが一般的であると考えられるが、フロッピーディスクや光ディスクなど、コンピュータ読みとり可能な記憶媒体であればどのようなものでも使用可能である。

【００７７】配列の内容

次に、上記配列管理モジュール１６で用いている配列の内容について説明する。

【００７８】図２には上記配列管理モジュール１６で用いている２種類の配列の内容を表す説明図が示されている。図２（１）には、個人情報管理配列２０ａが示されており、図２（２）には、暗号鍵管理配列２０ｂが示されている。

【００７９】図２（１）に示すように、個人情報管理配列２０ａは、ユーザの「ＩＤ」と、「登録動的署名データ」と、「鍵ハッシュ値」とを格納している配列である。この「鍵ハッシュ値」とは秘密鍵を、所定のハッシュ関数でハッシュ値に変換したものであり、このハッシュ値は、後述する暗号鍵管理配列２０ｂにおいて利用される。ハッシュ値を使用しているのは、上述したように秘密鍵の長さが５００ビット～１０００ビット程度であるため、秘密鍵の値そのもので配列の検索を行うと検索時間が長くなってしまうからである。

【００８０】さて、本実施の形態においては、ユーザを認識するためにそのユーザの「ＩＤ」を用いている（図２（１）参照）。そして、本実施の形態においては、１人のユーザが複数のＩＤを用いることを許容している。この結果、１人が複数の役職を有する場合に、各役職毎に異なる署名を１人のユーザが行うことが可能となる。

【００８１】本実施の形態において特徴的なことは、１人のユーザが複数のＩＤを用いることが、システム上許容されていることである。

【００８２】このような個人情報管理配列２０ａを用いているため、本実施の形態によれば、１人のユーザが複数の署名を使い分けることができ、利便性に富む署名処理を行うことができるのである。

【００８３】さらに、本実施の形態においては、１つの秘密鍵を複数のユーザが共有することを許容している。すなわち、異なるＩＤを有する異なる人に対して、同一の鍵ハッシュ値を割り当てることにより、一つの秘密鍵を複数人が共同で使用することが可能となる。

【００８４】例えば、上述した法人鍵等は複数人の取締役が使用する必要がある。そのような場合に、本実施の形態によれば、複数人の取締役が一つの法人鍵を共用することができるため、利便性の高いディジタル署名システムを実現することができる。

【００８５】もちろん、このコンピュータを複数人で共有し、複数人が１台のコンピュータを使用する場合においても、各ユーザが個別の秘密鍵を有する場合だけでなく、１つの共通の鍵を複数人全員で共有して使用することも可能である。

【００８６】図２（２）には、暗号鍵管理配列２０ｂが示されている。この図に示されているように、暗号鍵管

理配列２０ｂは、「鍵ハッシュ値」と、署名に用いる「秘密鍵」と、「クラス」が示されている。ここで、「鍵ハッシュ値」とは図２（１）で説明した鍵ハッシュ値であり、「クラス」とは秘密鍵の重要度を表すものであり、鍵を管理する際に用いられるデータである。このクラスは本発明にとっては必ずしも必須事項ではない。

【００８７】上述した個人情報管理配列２０ａを用いて、ユーザが使用する「ＩＤ」に従って、「鍵ハッシュ値」が求められる。この「鍵ハッシュ値」は、暗号鍵管理配列２０ｂの内容を検索する際にキーとして用いられる。暗号鍵管理配列２０ｂから、該当する「鍵ハッシュ値」が見いだされた場合には、対応する「秘密鍵」を暗号鍵管理配列２０ｂから得ることができる。

【００８８】このように、「鍵ハッシュ値」は、個人情報管理配列２０ａと、暗号鍵管理配列２０ｂとを結びつけるキーとしての役割を果たす。そのため、本実施の形態においては、「鍵ハッシュ値」を用いたが、秘密鍵と対応していれば、単なる連続番号をハッシュ値の代わりに用いるのも好ましい。

【００８９】また、本実施の形態においては、ＩＤに関して正規化された配列と、秘密鍵に関して正規化された配列と、の２種類の配列を使用して、個人の管理と鍵の管理をそれぞれ別個独立に行っている。すなわち、本実施の形態に係るディジタル署名生成方法を実現するプログラムを利用する者が増えた場合には、個人情報管理配列２０ａを調整し、秘密鍵の種類が減った場合等には、暗号鍵管理配列２０ｂのみを調整すればよく、効率の良い管理が行える。

【００９０】しかし、上述したように、配列管理モジュール１６の機能としては、ＩＤから、そのＩＤに対応する登録動的署名データ及び秘密鍵が求められれば、十分である。従って、個人情報管理配列２０ａと、暗号鍵管理配列２０ｂを統合して１つの配列を作り、その１つの配列で配列管理モジュール１６に関する処理を行うことも可能である。

【００９１】個人情報管理配列２０ａと暗号鍵管理配列２０ｂとを統合すると、「鍵ハッシュ値」が省略されて、ユーザの「ＩＤ」、「登録動的署名データ」、「秘密鍵」、「クラス」の各項目を有する配列が１つ作成されることになる。

【００９２】以上述べたように、本実施の形態において特徴的なことは、ディジタル署名に用いられる秘密鍵を集中的に管理するプログラムを設けており、特に、このプログラム中に配列の形で秘密鍵を保存したので、プログラムの作成者以外の者がこのプログラム中の秘密鍵を削除したり、新たに付加したり、改竄を加えることは著しく困難である。

【００９３】さらに、本実施の形態においては、本人であるかの特定のために生体署名データを使用した。そのため、本人であるとの特定をより正確なものとすることができるため、第三者によるいわゆる「なりすまし」等を防止することができる。

【００９４】そのため、本実施の形態に係るプログラムが第三者の手に渡っても、その第三者が悪意で秘密鍵を使用することはできず、また、プログラムの改竄による秘密鍵の悪用をすることも著しく困難となり、安全確実なディジタル署名を利用することができる。また、本実施の形態においては、複数人が１個の秘密鍵を共用すること、すなわち、１個の秘密鍵を複数人が共有することを許容しているため、法人鍵等の利用を円滑に行うことができる。更に、１人の人間が複数の秘密鍵を所有することをも許容しているため、役職毎に異なるディジタル署名をすることができる。

【００９５】以上述べたように、本実施の形態は、以下のような特徴を有する。

【００９６】（１）生体署名データを使用するため、各人は一般のパスワードより短い自己のＩＤのみを認識していれば秘密鍵の使用ができる。

【００９７】（２）各ユーザがタブレット上で手で書く署名を行うことにより各ユーザが本人であるかの特定を行っているため、紙を利用して行われていた従来の署名行為から円滑に移行することができる。

【００９８】（３）必要に応じて認証に用いた「手で書いた署名データ」のイメージデータを利用することができる。従って、既存の手で行っていた署名行為との整合性や類似性を保存する事ができる。

【００９９】

【発明の効果】以上述べたように本発明によれば、ユーザの特定を生体署名データで行ったため、本人の確認をより確実に行うことができる。

【０１００】また、本発明によれば、複数のユーザが１つの秘密鍵を共有できるため、いわゆる法人鍵の管理がし易くなり、また、代理署名等が容易になるという効果を奏する。

【０１０１】また、本発明によれば、１人のユーザが複数の秘密鍵を所有できるため、１人のユーザが役職に応じて複数のディジタル署名を使い分けることができるという効果を奏する。

【０１０２】また、本発明によれば、手で書く署名を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【０１０３】また、本発明によれば、網膜パターンを生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【０１０４】また、本発明によれば、指紋を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【０１０５】また、本発明によれば、手で書いた署名を表すイメージデータに対しても署名を施して出力するので、実際の手で書いた署名をイメージでとらえることが

できる。

【0106】また、本発明は、プログラムを格納したコンピュータ読みとり可能な記憶媒体であるため、秘密鍵の情報等をプログラム中に埋め込んで構成している。

【0107】したがって、本発明によれば、上で述べた各効果を奏すると共に、第三者にコピーされても未然に悪用を防止しうるという効果をも奏するのである。

【図面の簡単な説明】

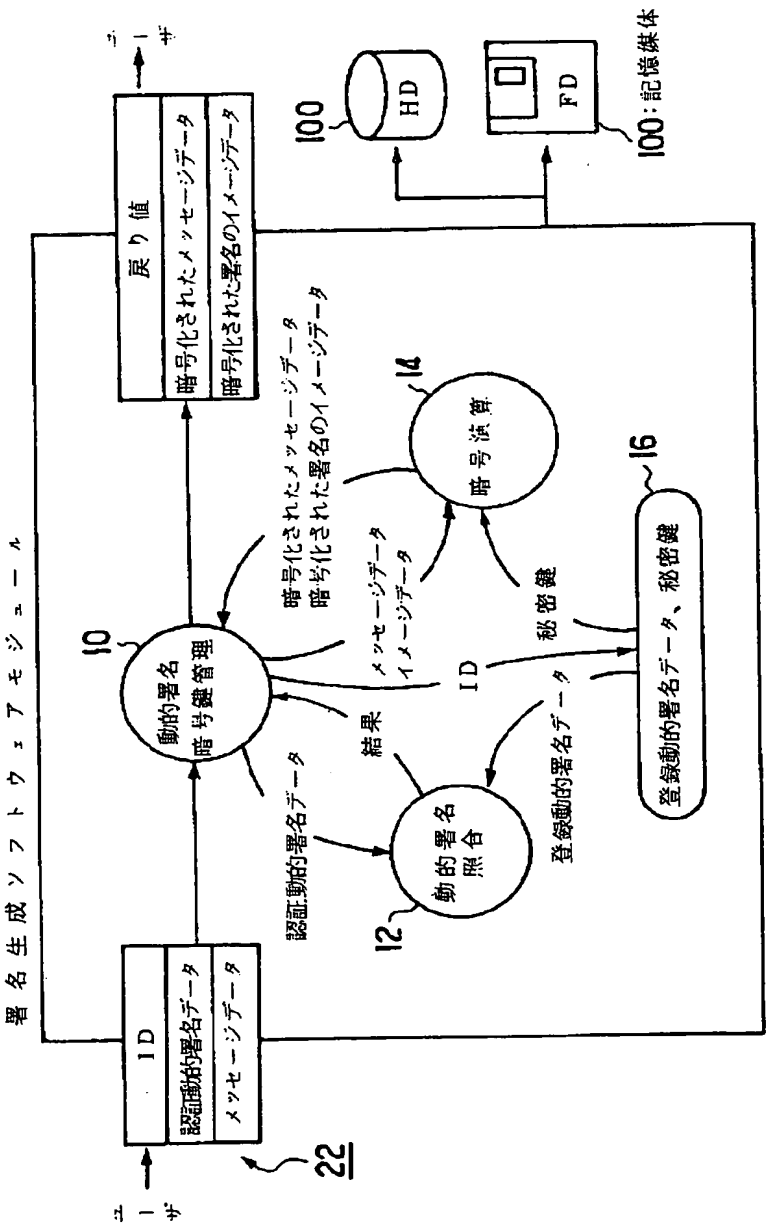
【図1】　本実施の形態に係るディジタル署名生成方法の構成を表す説明図である。

【図2】　図1の配列管理モジュールの配列を表す説明図である。

【符号の説明】

10　動的署名暗号鍵管理モジュール、12　動的署名照合モジュール、14暗号演算モジュール、16　配列管理モジュール、20a　個人情報管理配列、20b　暗号鍵管理配列、22　入力、100　記憶媒体。

【図1】



【図2】

個人情報管理配列

20a →

ID	登録動的署名データ	鍵ハッシュ値	

(1)

暗号鍵管理配列

20b ↓

鍵ハッシュ値	秘密鍵	クラス	

(2)